

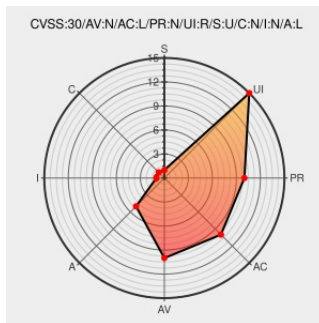


# CVE-2020-6342

Published on: 09/09/2020 12:00:00 AM UTC

Last Modified on: 12/02/2021 02:03:00 AM UTC

## CVE-2020-6342

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [3d Visual Enterprise Viewer](#) from [Sap](#) contain the following vulnerability:

SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated U3D file received from untrusted sources which results in crashing of the application and becoming temporarily unavailable until the user restarts the application, this is caused due to Improper Input Validation.

CVE-2020-6342 has been assigned by [sap](#) cna@sap.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [SAP](#) **SAP SE - SAP 3D Visual Enterprise Viewer** version **9**

CVSS3 Score: **4.3 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>LOW</b>          |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>PARTIAL</b>      |

## CVE References

| Description                    | Tags                                 | Link                     |
|--------------------------------|--------------------------------------|--------------------------|
| <b>No Description Provided</b> | <a href="#">Permissions Required</a> | <a href="#">SAP MISC</a> |

|                                                                                             |                                                                                  |                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                             | <a href="#">launchpad.support.sap.com</a><br>text/html                           | <a href="#">launchpad.support.sap.com/#/notes/2960815</a>                                                                                                                 |
| ZDI-20-1152   Zero Day Initiative                                                           | <a href="#">www.zerodayinitiative.com</a><br>text/html                           |  MISC<br><a href="#">www.zerodayinitiative.com/advisories/ZDI-20-1152/</a>             |
| SAP Security Patch Day – September 2020 - Product Security Response at SAP - Community Wiki | <a href="#">Vendor Advisory</a><br><a href="#">wiki.scn.sap.com</a><br>text/html |  MISC<br><a href="#">wiki.scn.sap.com/wiki/pages/viewpage.action?pagelId=557449700</a> |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type                                                                   | Vendor              | Product                                     | Version | Update | Edition | Language |
|------------------------------------------------------------------------|---------------------|---------------------------------------------|---------|--------|---------|----------|
| Application                                                            | <a href="#">Sap</a> | <a href="#">3d Visual Enterprise Viewer</a> | 9       | All    | All     | All      |
| Application                                                            | <a href="#">Sap</a> | <a href="#">3d Visual Enterprise Viewer</a> | 9       | All    | All     | All      |
| <a href="#">cpe:2.3:a:sap:3d_visual_enterprise_viewer:9:*:*:*:*:*:</a> |                     |                                             |         |        |         |          |
| <a href="#">cpe:2.3:a:sap:3d_visual_enterprise_viewer:9:*:*:*:*:*:</a> |                     |                                             |         |        |         |          |

No vendor comments have been submitted for this CVE

Social Mentions

| Source                                                            | Title | Posted (UTC) |
|-------------------------------------------------------------------|-------|--------------|
| <div><a href="#">← Previous ID</a><a href="#">Next ID →</a></div> |       |              |